

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK

JARRETT LEMIEUX,

Plaintiff,

v.

TARA LENICH; LU-SHAWN M.
THOMPSON, AS ADMINISTRATOR OF
ESTATE OF KENNETH P. THOMPSON;
ERIC GONZALEZ; MARK FELDMAN;
WILLIAM SCHAEFFER; BRIAN DONOHUE;
WILLIAM POWER; MICHAEL DOWLING;
JOSEPH PIRAINO; ROBERT KENAVAN; and
THE CITY OF NEW YORK,

Defendants.

**COMPLAINT &
JURY DEMAND**

— Civ. —

Plaintiff Jarrett Lemieux, by his attorneys, Wiggin and Dana LLP, alleges the following based on personal knowledge as to allegations regarding himself and on information and belief as to other allegations:

1. The Constitution of the United States and the Constitution of the State of New York protect certain bedrock rights from government intrusion, including the right to be free from unreasonable searches and seizures and the right to privacy. Perhaps the greatest invasion of these rights is the interception and monitoring of a person's private conversations.

2. For sixteen months, King's County Assistant District Attorney Tara Lenich invaded Plaintiff's privacy and violated his constitutionally and statutorily protected rights by illegally intercepting, monitoring, and recording all oral and electronic communications sent to and from his cellular telephone. She did so using her authority as Deputy Bureau Chief in Charge of Special Investigations in the King's County District Attorney's Office ("KCDA" or "the Office") and as a supervisor of the KCDA's wire room operations. She did so using the equipment, facilities, and funds

of the KCDA. And she did so in plain view of two District Attorneys and other supervisors within the KCDA, who allowed her to conduct a purported “confidential investigation” involving round-the-clock surveillance of Plaintiff’s cell phone for well over a year, despite knowing that no such confidential investigation ever existed.

3. Lenich could never have conducted this illegal wiretapping operation, but for a municipal policy or custom of deliberate indifference toward the oversight of wiretaps within the KCDA. State and federal law impose stringent requirements on law-enforcement agencies conducting wiretaps, including detailed requirements on the content and form of applications for wiretap authorizations, limits on the length of time a wiretap can remain operative, and strict record-keeping and reporting requirements. These state and federal requirements and limitations exist precisely to avoid the foreseeable risk that a law enforcement officer might abuse his or her authority and engage in eavesdropping or other invasions of privacy. Nevertheless, consistent with the KCDA’s policy and custom of deliberate indifference, Lenich’s supervisors turned a blind eye as she submitted no fewer than *seventeen* obviously forged wiretap orders and carried out a purported “confidential” surveillance operation for well over a year.

4. Lenich’s scheme would have been easily detected within the first month had her supervisors complied with their obligations under state and federal law to keep records of all KCDA wiretaps for the purpose of reporting statistics to the Administrative Office of United States Courts. However, while the Administrative Office Wiretap Reports for 2014 and 2017 reflect data presumably submitted by the KCDA, the Administrative Office Wiretap Reports for 2015 and 2016 indicate that “[n]o prosecutor’s report” was received in those years—the two years during which Lenich carried out her scheme.

5. The invasion of Plaintiff’s privacy was compounded by the fact that Lenich not only intercepted and eavesdropped on Plaintiff’s private communications, but also disclosed information

gleaned from those interceptions to others for the purpose of harassing Plaintiff and undermining his relationships with others in the KCDA and New York Police Department (NYPD). Others in the KCDA willingly spread rumors involving Plaintiff that found their origins in illegally intercepted conversations.

6. When, well over a year after it had begun, the illegal wiretap campaign was finally uncovered, other KCDA supervisors and employees further violated Plaintiff's federally protected rights by using and disclosing Plaintiff's private communications despite knowing that they had been illegally intercepted. Plaintiff's name was leaked to the press, along with false and/or misleading information about him, leading to days of invasive media coverage and further intrusion into Plaintiff's private life.

7. While Lenich was arrested, charged, and convicted for violating the Wiretap Act, Plaintiff has not been compensated for the serious injuries he suffered as a result of the illegal wiretap operation. On the contrary, despite the fact that he is a victim of a serious crime, Plaintiff has been treated like a pariah. When news of Lenich's illegal conduct came to light on or about November 28, 2016, Plaintiff's supervisors responded by reassigning Plaintiff from the elite ATF-NYPD Joint Firearms Task Force on which he had served to modified duty. Defendant Mark Feldman, a supervisor in the KCDA, went so far as to order Plaintiff not to enter the KCDA again and request that Plaintiff's supervisors in the NYPD remove him from KCDA assignments. Plaintiff was relegated to a desk job without the privileges and opportunities for overtime that he had previously enjoyed.

8. Plaintiff has been severely harmed by the Defendants' illegal and wrongful acts and omissions. Most obviously, as a result of the illegal wiretap campaign and the disclosure of his private communications, Plaintiff suffered severe embarrassment and reputational harm and continues to suffer from anxiety and emotional distress stemming from this grievous invasion of his privacy. Moreover, as a result of the punitive response to his victimization, Plaintiff has suffered tangible

professional consequences. For almost a year, he was prevented from earning overtime and nightshift pay, resulting in lost earnings and a potential negative impact on future earnings and/or pension benefits. Finally, his once-bright prospects for substantial earnings in the private sector following his retirement have been harmed due to the reputational injuries he has suffered as a result of Defendants' acts and omissions.

9. Plaintiff now seeks redress under the Wiretap Act, the Stored Communications Act, the United States Constitution, and state common law against Lenich, the City of New York, and the KCDA supervisors and employees who permitted or actively participated in the invasion of Plaintiff's privacy and punished him for being the victim of a crime.

PARTIES

10. Plaintiff Jarrett Lemieux is a United States citizen and is a resident of Nassau County, New York.

11. At all relevant times, Defendant Tara Lenich was the Deputy Chief of Special Investigations of Violent Criminal Enterprises at the KCDA, acting in the capacity of agent, servant, and employee of Defendant City of New York, within the scope of her employment as such, and acting under color of State law. Lenich was responsible for the policy, practice, and supervision of KCDA wiretap operations and oversaw KCDA wiretaps in connection with firearms, narcotics, vice, and gang investigations. She is sued in her individual capacity.

12. Defendant Lu-Shawn M. Thompson is a citizen and resident of New York. She is the Administrator of the Estate of Kenneth P. Thompson, who is deceased. From 2014 until his death on October 9, 2016, Kenneth Thompson was the District Attorney for Kings County, acting in the capacity of agent, servant, and employee of Defendant City of New York, within the scope of his employment as such, and acting under color of state law. Mr. Thompson was responsible for the policy, practice, supervision, implementation and conduct of all KCDA matters and was responsible

for the training, supervision and conduct of all KCDA personnel, including Ms. Lenich and the other individual defendants. Lu-Shawn Thompson, as Administrator of the Estate of Kenneth Thompson, is sued for the acts and omissions of Kenneth Thompson undertaken in his individual capacity.

13. Defendant Eric Gonzalez is a citizen and resident of New York. From 2014 until approximately October 9, 2016, Mr. Gonzalez was the Deputy District Attorney for the KCDA; from October 9, 2016, until approximately January 21, 2018, Mr. Gonzalez was the Acting District Attorney for Kings County; since January 21, 2018, Mr. Gonzalez has been the District Attorney for Kings County. In all three roles, Mr. Gonzalez acted in the capacity of agent, servant, and employee of Defendant City of New York, within the scope of his employment as such, and acting under color of state law. Mr. Gonzalez was responsible for the policy, practice, supervision, implementation and conduct of all KCDA matters and was responsible for the training, supervision and conduct of all KCDA personnel, including Ms. Lenich and the other individual defendants. Mr. Gonzalez is sued in his individual capacity.

14. Defendant William Schaeffer is a citizen and resident of New York. At all relevant times, Mr. Schaeffer was an Executive Bureau Chief within the KCDA, acting in the capacity of agent, servant, and employee of Defendant City of New York, within the scope of his employment as such, and acting under color of state law. Mr. Schaeffer was responsible for the policy, practice, supervision, implementation and conduct of KCDA matters and was responsible for the training, supervision, and conduct of KCDA personnel, including Ms. Lenich. Mr. Schaeffer is sued in his individual capacity.

15. Defendant Mark Feldman is a citizen and resident of New York. At all relevant times, Mr. Feldman was on the executive team for the KCDA's office, either acting as Chief Assistant District Attorney or in his current role as Executive Assistant District Attorney for Crime Strategies. In those roles, he acted in the capacity of agent, servant, and employee of Defendant City of New York, within

the scope of his employment as such, and under color of state law. Mr. Feldman is sued in his individual capacity.

16. Defendant Brian Donohue is a citizen and resident of New York. At all relevant times, Mr. Donohue was an Assistant Deputy Chief Investigator within the KCDA, acting in the capacity of agent, servant, and employee of Defendant City of New York, within the scope of his employment as such, and acting under color of state law. Mr. Donohue was responsible for reviewing all judicial orders authorizing the KCDA to conduct wiretaps to ensure they were authentic and for the day-to-day oversight of KCDA's wire rooms. Mr. Donohue was also responsible for physically establishing the wiretaps in a designated, controlled location. Mr. Donohue was also a designated "system administrator" with access to the KCDA's wiretap servers, which stored the oral and wire communications that were intercepted during the illegal wiretap operation. Mr. Donohue is sued in his individual capacity.

17. Defendant William Power is a citizen and resident of New York. At all relevant times, Mr. Power was KCDA's Chief Information Officer, acting in the capacity of agent, servant, and employee of Defendant City of New York, within the scope of his employment as such, and acting under color of state law. Mr. Power was a designated "system administrator" with access to the KCDA's wiretap servers, which stored the oral and wire communications that were intercepted during the illegal wiretap operation. He is sued in his individual capacity.

18. Defendant Michael Dowling is a citizen and resident of New York. At all relevant times, Mr. Dowling was a Detective Investigator in the KCDA, acting in the capacity of agent, servant, and employee of Defendant City of New York, within the scope of his employment as such, and acting under color of state law. Mr. Dowling was a designated "system administrator" with access to the KCDA's wiretap servers, which stored the oral and wire communications that were intercepted during the illegal wiretap operation. He is sued in his individual capacity.

19. Defendant Joseph Piraino is a citizen and resident of New York. At all relevant times, Mr. Piraino was a Chief Investigator in the KCDA, acting in the capacity of agent, servant, and employee of Defendant City of New York, within the scope of his employment as such, and acting under color of state law. Mr. Piraino was a designated “system administrator” with access to the KCDA’s wiretap servers, which stored the oral and wire communications that were intercepted during the illegal wiretap operation. He is sued in his individual capacity.

20. Defendant Robert Kenavan is a citizen and resident of New York. At all relevant times, Mr. Kenavan was a Detective Investigator in the KCDA acting in the capacity of agent, servant, and employee of Defendant City of New York, within the scope of his employment as such, and acting under color of state law. Mr. Kenavan was a designated “system administrator” with access to the KCDA’s wiretap servers, which stored the oral and wire communications that were intercepted during the illegal wiretap operation. He is sued in his individual capacity.

21. Defendant City of New York (the City) is a municipal corporation that is responsible for the disciplinary, management, and administrative practices of the KCDA. The KCDA, through its senior officials, promulgates and implements administrative policies, including those with respect to applications for wiretaps and the operation of wiretaps. The City is sued directly under 18 U.S.C. §§ 2520 and 2707 and as principal for the acts of its employees, including Lenich, within the scope of their employment.

22. Defendants Thompson, Gonzalez, Schaeffer, and Feldman are collectively referred to as the “Supervisory Defendants.”

23. Defendants Donohue, Power, Dowling, Piraino, and Kenavan are collectively referred to as the “Administrator Defendants.”

24. The Supervisory Defendants and the Administrator Defendants are collectively referred to as the “Individual Defendants.”

JURISDICTION & VENUE

25. This Court has jurisdiction over this case pursuant to 28 U.S.C. § 1331, because the action arises under 18 U.S.C. §§ 2510, *et seq.*, 18 U.S.C. §§ 2701, *et seq.*, 42 U.S.C. §§ 1983 & 1988, and the Fourth and Fourteenth Amendment of the United States Constitution.

26. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b), because the acts complained of occurred in the Eastern District of New York.

JURY DEMAND

27. Plaintiff demands trial by jury.

FACTUAL ALLEGATIONS

Plaintiff's Work at the New York City Police Department

28. Plaintiff joined the New York City Police Department ("NYPD") on July 2, 2001.

29. Plaintiff has excelled in his work and, up until his name was dragged through the mud as a result of Defendants' tortious acts, he had a sterling reputation as a detective in the NYPD.

30. After joining the NYPD in July 2001, Plaintiff quickly rose through the ranks, earning several discretionary promotions. He was promoted to Detective Third Grade in May 2006, to Detective Second Grade in May 2012, and in March 2015, he was promoted to Detective First Grade, an elite designation for the NYPD's most senior and experienced investigators.

31. As a detective, Plaintiff has developed a particular expertise in investigating narcotics and firearms trafficking. Early in his career, Plaintiff was recruited to join an elite NYPD-ATF Firearms Task Force formed to investigate illegal firearm trafficking. Being part of this joint federal-state task force was not only a prestigious honor; it came with material benefits, including a take-home vehicle and significant opportunities for overtime pay.

32. Plaintiff has participated in, and led, some of the NYPD's most sensitive and important investigations, including "Operation Far From Home," which uncovered a high-volume Florida-to-

Brooklyn gun-trafficking ring, and “Operation Sesame Street,” which uncovered a gun-running ring run by Delta Airlines baggage handlers. As a result of these and other investigations, Plaintiff has helped to take hundreds of illegal firearms off the streets of New York City.

33. Plaintiff worked directly with Defendant Lenich on numerous investigations beginning in 2005, including the Delta Airlines case. At all times that Plaintiff worked with Lenich, she was the Deputy Chief of Special Investigations of Violent Criminal Enterprises, a unit within the KCDA.

Conducting a Wiretap at KCDA

34. At all relevant times, any KCDA Assistant District Attorney (ADA) seeking to conduct a wiretap was required to file a wiretap application with a court of competent jurisdiction, along with an affidavit demonstrating the requisite probable cause and need for a wiretap.

35. KCDA policy requires that a supervisor, such as Lenich, approve these wiretap applications.

36. As a matter of custom or policy, once an order authorizing a wiretap is signed by a judge, the order is given to Defendant Donohue, an Assistant Deputy Chief Investigator, who is responsible for ensuring that the order is authentic and properly signed. As part of this review, Donohue was supposed to look for a raised judicial seal which, while not required, is standard on valid orders as a means of demonstrating their authenticity.

37. Only those individuals named in an order authorizing a wiretap are permitted to review the communications that are intercepted through the wiretap. A wiretap order typically authorizes a minimum of two ADAs, as well as all of the supervisors above those ADAs in the chain of command, to review the intercepted communications. A wiretap order also typically authorizes identified law enforcement personnel who have been specifically trained on the parameters and requirements of the governing order to monitor and minimize intercepted communications.

38. In addition to authorized ADAs, the Administrator Defendants—Donohue, Power, Dowling, Piraino, and Kenavan—have continuous access to the KCDA wiretap servers and therefore have the ability to listen to intercepted recordings.

39. Before Lenich was promoted to Deputy Chief of Special Investigations of Violent Criminal Enterprises, KCDA wiretap operations were generally facilitated by the New York Police Department's Tactical Action Response Unit out of a clandestine NYPD location in Queens.

40. In or around 2013, Lenich caused Defendant Thompson to invest funds to create separate "wire room" facilities, containing all necessary equipment, within the KCDA office at 350 Jay Street, so that she and other ADAs could conduct wiretap operations without the necessity of involving members of the NYPD Tactical Action Response Unit.

41. Wiretaps conducted by the KCDA are paid for out of City funds. Although personnel costs account for much of the expense of a wiretap, there are also costs associated with the running of equipment and with fees charged by the service providers that facilitate the interceptions. Service fees are significant and are typically charged for each month that a wiretap is active.

42. KCDA wiretap operations must comply with state and federal law.

43. The federal Wiretap Act provides precise procedures that law enforcement officers must follow in order to obtain an order authorizing or approving the interception of wire, oral, or electronic communications.

44. Subject to narrow exceptions, each application for a wiretap order *must* include:

- a. the identity of the investigative or law enforcement officer making the application, and the officer authorizing the application;
- b. a full and complete statement of the facts and circumstances relied upon by the applicant to justify his or her belief that an order should be issued;

- c. a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous;
- d. a statement of the period of time for which the interception is required to be maintained, including a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter; and
- e. a full and complete statement of the facts concerning all previous applications made to any judge for authorization to intercept communications involving any of the same persons, facilities or places specified in the application.

18 U.S.C. § 2518(1). New York's analogous wiretap statute contains similar requirements. N.Y. Crim. Pro. L. § 700.20.

45. A judge may enter an order authorizing or approving interception of wire, oral, or electronic communications under the Wiretap Act or New York's wiretap statute only if the judge determines that:

- a. there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular enumerated offense;
- b. there is probable cause for belief that particular communication concerning that offense will be obtained through such interception;
- c. normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous; and
- d. there is probable cause for belief that the facilities from which, or the place where, the communications are to be intercepted are being used, or are about to be used, in connection with the commission of the offense, or are leased to, listed in the name of, or commonly used by such person.

28 U.S.C. § 2518(3); N.Y. Crim. Pro. L. § 700.

46. A valid wiretap order may not authorize or approve the interception of any wire, oral, or electronic communication for any period longer than is necessary to achieve the objective of the authorization, and in no event may a wiretap be authorized for longer than thirty days. 28 U.S.C. § 2518(5); N.Y. Crim. Pro. L. § 700.10. An application for an extension of a wiretap order must set forth the results thus far obtained from the interception in addition to the other required statements referenced above in Paragraph 43. 28 U.S.C. § 2518(3); N.Y. Crim. Pro. L. § 700.20.

47. The Wiretap Act requires district attorneys to keep detailed records on the use of wiretaps and to file annual reports with the Administrative Office of the United States Courts. By law, district attorneys must file reports in March of each year containing the following information with respect to each application for an order or extension made in the preceding calendar year:

- a. the fact that an order or extension was applied for;
- b. the kind of order or extension applied for;
- c. the fact that the order or extension was granted as applied for, was modified, or was denied;
- d. the period of interceptions authorized by the order, and the number and duration of any extensions of the order;
- e. the offense specified in the order or application, or extension of an order;
- f. the identity of the applying investigative or law enforcement officer and agency making the application and the person authorizing the application;
- g. the nature of the facilities from which or the place where communications were to be intercepted;
- h. a general description of the interceptions made under each order or extension, including (i) the approximate nature and frequency of incriminating communications

intercepted; (ii) the approximate nature and frequency of other communications intercepted; (iii) the approximate number of persons whose communications were intercepted; (iv) the number of orders in which encryption was encountered and whether such encryption prevented law enforcement from obtaining the plain text of communications intercepted pursuant to such order; and (v) the approximate nature, amount, and cost of the manpower and other resources used in the interception;

- i. the number of arrests resulting from interceptions made under each order or extension, and the offenses for which arrests were made;
- j. the number of trials resulting from such interceptions;
- k. the number of motions to suppress made with respect to such interceptions, and the number granted or denied; and
- l. the number of convictions resulting from such interceptions and the offenses for which the convictions were obtained and a general assessment of the importance of the interceptions.

18 U.S.C. § 2519(2). Under State law, “each district attorney” must submit the report required by federal law in January of each year. N.Y. Crim. Pro. L. § 700.60.

48. Notwithstanding this requirement of state and federal law, the Administrative Office Wiretap Reports for Calendar Years 2015 and 2016—the two years during which Lenich carried out the illegal wiretap operation—indicate that “[n]o prosecutor’s report” was received from KCDA. The Administrative Office Wiretap Reports for the years immediately preceding and following Calendar Years 2015 and 2016 do contain information reported by the KCDA.

49. The Administrative Office of United States Courts assembles the data reported annually by courts and prosecutors and publishes statistics on state and federal wiretaps. According to these published reports, during Calendar Year 2016, there were 3,168 reported wiretap orders in the United

States. The average length of an authorized wiretap was 44 days. In Calendar Year 2015, there were 4,418 reported wiretap orders. The average length of an authorized wiretap was 43 days.

50. By comparison, the wiretap on Plaintiff's personal cell phone described in this Compliant lasted approximately 484 days in 2015 and 2016, more than ten times longer than the average wiretap in those years.

Lenich Uses KCDA Equipment, Facilities, and Personnel to Conduct a Sweeping Wiretap Operation on Plaintiff's Private Cellular Phone

51. From approximately June 2015 through November 28, 2016, Lenich conducted an illegal wiretap operation on the cellular phones of Plaintiff and another victim, Stephanie Rosenfeld, who was an Assistant District Attorney in the KCDA.

52. Lenich illegally intercepted, recorded, and monitored the oral and electronic communications sent to and from the cell phone of Stephanie Rosenfeld from approximately June 2015 through December 2015.

53. Lenich illegally intercepted, recorded, and monitored the oral and electronic communications sent to and from Plaintiff's cell phone from approximately August 2015 through November 28, 2016.

54. Lenich's illegal wiretap campaign was not sophisticated. She used a rudimentary "cut and paste" method to replicate the signatures of various New York State Supreme Court Justices on documents purporting to be court orders, by physically cutting a copy of each judge's signature from a legitimate document and taping it onto the fraudulent documents she had created.

55. Lenich then presented the fraudulent documents to Defendant Donohue, who reviewed and accepted them. Though none of the forged orders Lenich showed to Defendant Donohue had original signatures or a raised judicial seal, Donohue nevertheless approved them and sent the forged orders (or caused them to be sent) to Plaintiff's cell phone provider and to Ms. Rosenfeld's cell phone provider.

56. Each forged order submitted to the cell phone providers purported to authorize the KCDA to intercept and record the oral and electronic communications transmitted to and from Plaintiff's cell phone or Ms. Rosenfeld's cell phone for a period of 30 days.

57. At the end of each 30-day period, Lenich created a new forged order using the same rudimentary "cut and paste" method, and Defendant Donohue sent the new forged order (or caused it to be sent) to the cell phone providers, purporting to authorize the continued interception and recording of the communications transmitted to and from Plaintiff's cell phone or Rosenfeld's cell phone for an additional 30 days.

58. Lenich, facilitated by Donohue, submitted approximately seventeen forged judicial orders to Plaintiff's cell phone provider, resulting in the continuous, round-the-clock, interception and recording of all electronic and oral communications to and from Plaintiff's cell phone for a period of approximately sixteen months, or 484 days.

59. Lenich, facilitated by Donohue, submitted approximately seven forged judicial orders to Ms. Rosenfeld's cell phone provider, resulting in the continuous, round-the-clock, interception and recording of all electronic and oral communications to Ms. Rosenfeld's cell phone for a period of approximately seven months, or 213 days.

60. The total duration of the illegal wiretap campaign on the two victims' cell phones was approximately eighteen months, or 545 days.

61. Upon information and belief, Lenich also used a fraudulent search warrant to obtain access to Plaintiff's cell phone provider and obtain and review text messages and emails that were sent to or from Plaintiff's cell phone and stored with Plaintiff's cell phone provider.

62. During the approximately 484 days that his cell phone was illegally wiretapped, all oral and electronic communications to and from Plaintiff's phone were intercepted, recorded, and stored

on KCDA servers that were accessible to the Individual Defendants and others with access to the wiretap servers.

63. During this time, Plaintiff used his cell phone to communicate with his wife, his children, other family members, and friends. He also used his cell phone to communicate with colleagues and informants that were employed by the NYPD to further a variety of investigations. Lenich contemporaneously intercepted and recorded all of these private and confidential communications using KCDA equipment and facilities.

64. Neither Plaintiff nor any party to Plaintiff's private communications consented to having those communications intercepted or recorded.

65. Plaintiff also communicated with Ms. Rosenfeld via her cell phone during the period of time in which it was illegally wiretapped. Neither Plaintiff nor Ms. Rosenfeld consented to those private communications being intercepted or recorded.

66. Lenich used information illegally intercepted from Plaintiff's cell phone to harass and intimidate him and to undermine his relationships with other colleagues in the NYPD and KCDA, including his partner and immediate supervisor.

67. Upon information and belief, Lenich disclosed the substance of Plaintiff's private communications to KCDA employees and others, including the Individual Defendants.

Plaintiff is Subjected to Further Invasions of Privacy when KCDA Employees Leak Details about the Illegal Wiretap Operation to the Press

68. The illegal wiretap campaign ended on or about November 28, 2016, when KCDA filed a criminal complaint in Kings County Criminal Court charging Lenich with two counts of eavesdropping under New York Penal Law § 250.05 and two counts of criminal possession of a forged instrument in the second degree under New York Penal Law § 170.24.

69. Plaintiff only learned that his private communications had been illegally intercepted and recorded after Lenich had been arrested.

70. Upon information and belief, the Supervisory Defendants all knew prior to November 28, 2016, that Lenich had intercepted Plaintiff's private communications and that Plaintiff's private communications were stored on Lenich's laptop computer.

71. Rather than arrest Lenich immediately, the Supervisory Defendants allowed her to have continued access to Plaintiff's private communications and allowed her the opportunity to potentially delete or destroy evidence and to continue to disclose illegally obtained private communications.

72. Lenich's arrest was covered extensively in the media. Plaintiff's name was leaked to the media, which reported that one of the phones that Lenich illegally intercepted belonged to him. The media also reported that Plaintiff had been put on "desk duty" as a result of a threatening statement he purportedly made to Lenich that was recorded by the wiretap.

73. Upon information and belief, one or more of the Individual Defendants—who were among the only individuals with access to the KCDA wiretap servers—was the source of these leaks.

74. As a result of these disclosures to the media, Plaintiff's name appeared in multiple news sources for weeks. Reporters staked out his house and accosted him and his family in an effort to obtain more information about the illegal wiretapping campaign.

75. On or about March 23, 2017, a federal grand jury indicted Lenich on two counts of illegal interception of communications in violation of 18 U.S.C. §§ 2511(1)(a), 2511(4)(a) and 3551, et seq.

76. On April 3, 2017, Lenich pleaded guilty to the indictment. She was sentenced on February 2, 2018, to one year and one day imprisonment.

77. Lenich is currently serving her sentence.

The Individual Defendants Use and Disclose Plaintiff's Private Communications

78. The Individual Defendants each had access to the KCDA servers on which Plaintiff's unlawfully intercepted communications were stored.

79. The Administrator Defendants were designated system administrators with continuous access to the KCDA wiretap servers, including recordings of communications intercepted by the illegal wiretaps. The Supervisory Defendants had access to the KCDA wiretap servers in their supervisory capacity.

80. After Lenich's misconduct came to light, the Individual Defendants were directly involved in the KCDA investigation of the operation and therefore had continued access to the illegally intercepted communications.

81. The Individual Defendants each received, used, reviewed, and/or disclosed copies of telephonic and electronic communications that were unlawfully intercepted from Plaintiff's cell phone and Ms. Rosenfeld's cell phone.

82. The Individual Defendants knew Plaintiff's communications had been unlawfully obtained at the time they received, used, reviewed, and/or disclosed them.

83. The Individual Defendants used Plaintiff's private, unlawfully obtained communications and disclosed them to one another, as well as to others, without Plaintiff's permission.

84. Neither Plaintiff nor any party to the intercepted communications consented to anyone from the KCDA using or disclosing Plaintiff's private communications.

85. Following Lenich's arrest on November 28, 2016, KCDA employees talked about the communications that had been unlawfully intercepted.

86. Characterizations of the contents of communications that were unlawfully intercepted from Plaintiff's cellular phone were splattered across the media, even though the contents of those communications should never have been disclosed.

87. In or about December 2016, Plaintiff's counsel spoke to Defendant Schaeffer, who gave assurances that the illegally obtained recordings of Plaintiff's communications would be placed under seal and not further disclosed.

88. On December 21, 2016, Plaintiff's counsel sent a letter to Patricia McNeill, Deputy Chief of Investigations at KCDA, confirming that Schaeffer gave these assurances and reiterating Plaintiff's request that the KCDA keep the illegally obtained recordings under seal as required by law.

89. Upon information and belief, Plaintiff's illegally intercepted communications were never properly sealed.

90. Upon information and belief, despite Defendant Schaeffer's assurances, the Supervisory Defendants retained a copy of Plaintiff's illegally obtained private communications even after the DOJ assumed control over the Lenich prosecution and certain KCDA employees listened to the recordings without properly unsealing them or notifying Plaintiff and giving him the opportunity to object to the fact that his private communications would be further disclosed.

91. Upon information and belief, the Individual Defendants were among those who listened to and reviewed the recordings of Plaintiff's communications, despite knowing they had been obtained illegally. They did so without notifying Plaintiff and giving him the opportunity to object.

92. Upon information and belief, and despite Schaeffer's assurances, in or around January 2018, KCDA employees reviewed and then disclosed nearly 200 hours of Plaintiff's private communications to a Justice of the New York Supreme Court who was presiding over the Delta Airlines gun-running case. They did so without providing notice to the Plaintiff, seeking Plaintiff's authorization, or providing Plaintiff with an opportunity to be heard. Upon information and belief, the Individual Defendants were among those who reviewed and disclosed the communications, knowing that they had been obtained illegally. Upon information and belief, the Supervisory Defendants authorized the review and subsequent disclosure of Plaintiff's private communications despite their knowledge that Plaintiff's private communications had been obtained illegally.

93. In February 2018, at a hearing in which Plaintiff, through his counsel, contested the proposed in camera review by a Justice of the New York Supreme Court of approximately 200 hours

of these recordings, Plaintiff learned for the first time that not only had KCDA employees reviewed the contents of the illegally obtained recordings without his authorization, but they had further disclosed the contents of at least one recorded conversation to defense lawyers in the Delta Airlines case, without notifying Plaintiff or giving him the opportunity to object.

94. After learning that Defendant Schaeffer had not followed through with his promise to seal and not further disclose the illegally obtained recordings, Plaintiff's counsel sent a letter to KCDA. In that letter, Plaintiff's counsel requested that the KCDA (inter alia):

- a. Provide a full accounting of any and all uses, duplications, and disclosures of the recordings of Plaintiff's private communications, including the whereabouts of any and all copies of said recordings, the names of any and all individuals within the KCDA's office who have handled the recordings, and the names of any and all persons who have listened to any portion of the recordings;
- b. Provide copies of any and all motions, filings, orders, or other requests to review, disclose, or duplicate any portion of the illegally obtained recordings;
- c. Provide copies of any and all orders, including supporting documents, that Lenich or any other member of the KCDA's office used to obtain and record Plaintiff's private communications;
- d. Provide copies of the results of any internal investigation into this matter and all documentation supporting any such investigation; and
- e. Retrieve and destroy all known copies of Plaintiff's illegally obtained private communications, whether currently or formerly in the possession of the KCDA's office.

95. Defendant Schaeffer and the other Supervisory Defendants refused to comply with the requests in Plaintiff's April 11 letter and, upon information and belief, the KCDA continues to maintain copies of Plaintiff's private communications.

The City's Liability for the Illegal Wiretap Campaign

96. The City is liable for Lenich's actions because she conducted the illegal wiretap Campaign within the scope of her employment by the City; because she was a final policymaker with authority to establish municipal policy with respect to KCDA wiretap operations; and because her misconduct was directly enabled and facilitated by a municipal policy of deliberate indifference toward KCDA wiretap operations.

97. As the Deputy Chief of Special Investigations of Violent Criminal Enterprises and a supervisor of the wiretap room facilities, Lenich had broad authority to initiate and oversee wiretaps and she routinely conducted wiretap operations without oversight or supervision.

98. Lenich conducted the illegal wiretap campaign on KCDA premises, and using KCDA equipment and facilities. The costs of the wiretap campaign were paid out of KCDA funds on a monthly basis.

99. Lenich conducted the illegal wiretap campaign, by her own account, at least in part for the benefit of the KCDA. During most of the period of time that the illegal wiretap campaign was ongoing, Lenich was working closely with Plaintiff on a major criminal investigation, the Delta Airlines case. At her sentencing, she testified that part of her motivation in eavesdropping on Plaintiff's conversations was that she was "trying to protect" her work on that case, which was "the biggest case of [her] career."

100. Lenich's misconduct was reasonably foreseeable because she had a past history of abusing her authority within the KCDA and had virtually limitless authority to conduct wiretaps. Upon information and belief, Lenich was the subject of multiple EEOC complaints from fellow ADAs

during the period in which she was conducting the unlawful wiretaps, about which the Supervisory Defendants knew or should have known. Upon information and belief, these complaints detailed erratic and incendiary behavior. As a result of these complaints, upon information and belief, Lenich was ordered by her superiors to undergo specialized counseling. In addition, it was widely known that Lenich was responsible for causing KCDA to establish its own wire room facilities, thereby bypassing the participation of the NYPD Tactical Action Response Unit.

101. The City is also liable for Lenich's misconduct because she was a final policymaker with final authority to establish municipal policy with respect to KCDA wiretap operations.

102. In her capacity as Deputy Chief of Special Investigations of Violent Criminal Enterprises, Lenich had the authority to report and make requests directly to Defendants Thompson and Gonzalez, without going through others in the chain of command.

103. She demonstrated her authority over KCDA wiretapping operations by, among other things, causing KCDA to establish wire room facilities within its office in Brooklyn, bypassing the participation of the NYPD Tactical Action Response Unit.

104. As Deputy Chief of Special Investigations of Violent Criminal Enterprises, Lenich supervised ADAs and detectives who conducted investigations within the KCDA and who installed wiretaps, including Defendant Donohue. Lenich had primary control over wiretap operations stemming from narcotics, firearms, vice, and gang investigations, with final policymaking authority with regard to whether to seek a wiretap, how to establish a wiretap, and how to execute an order for a wiretap.

105. If Lenich were not a final policymaker, she would not have been able to establish and maintain an eighteen-month-long "confidential" wiretap operation without interference from other KCDA supervisors.

106. The City is also liable for Lenich's misconduct because it was enabled and facilitated by a municipal policy or custom of deliberate indifference to the operation of KCDA wiretaps.

107. The Supervisory Defendants, who were final policymakers for the City, acting within the scope of their employment as agents of the City, knew or should have known that Lenich was acting without oversight or supervision with respect to KCDA wiretaps.

108. All told, between June 2015 and November 28, 2016, Lenich forged approximately twenty-four judicial orders. Not one of these orders contained an original signature or raised seal. Nevertheless, Defendant Donohue approved and sent (or caused to be sent) each and every one of the forged orders to Ms. Rosenfeld's and Plaintiff's cell phone providers, purporting to authorize a continuous, round-the-clock wiretap campaign on each of their cell phones for nearly a year and a half.

109. Though Lenich claimed, for approximately eighteen months, that she was conducting a "confidential" investigation, the Supervisory Defendants knew or should have known that no such investigation existed.

110. Upon information and belief, the Supervisory Defendants were aware of Lenich's illegal wiretap campaign as evidenced by the fact that they were required by state and federal law to keep detailed records on KCDA wiretap operations, including information on the length of interceptions and the number and duration of any extension; descriptions of the interceptions, and the number of arrests resulting from the interceptions. It is inconceivable that the Supervisory Defendants could have maintained this information without realizing that Lenich was conducting an unauthorized and illegal wiretap operation.

111. Despite the reporting requirements of state and federal law, the Administrative Office Wiretap Reports for Calendar Years 2015 and 2016 indicate that "[n]o prosecutor's report" was submitted from KCDA for the two years during which the illegal wiretap operation transpired.

112. The Administrative Office Wiretap Reports do reflect data provided by the KCDA for Calendar Years 2013 and 2014, before the illegal wiretapping operation commenced. In 2013, the KCDA reported 6 installed wiretaps with an average of 2.3 extensions per wiretap and an average total duration of 85.7 days. In 2014, the KCDA reported 61 installed wiretaps, with an average of 1.4 extensions per wiretap and an average total duration of 61.6 days.

113. Had Defendants Thompson and Gonzalez complied with their statutory reporting obligation in 2015 and 2016, the data reported to the Administrative Office would have included at least two installed wiretaps that were not reflected in the corresponding data on judicially authorized wiretaps for KCDA that is separately reported by state and federal judges. KCDA's data for 2015 and 2016 would also have reflected that one of these wiretaps (which took place entirely in Calendar Year 2015) was extended six times and lasted approximately 213 days and the other (which began in August 2015 and continued through November 2016) was extended sixteen times and lasted approximately 484 days, far above the average number of extensions and total duration for the preceding two years.

114. Had Defendants Thompson and Gonzalez complied with their statutory reporting obligations in 2015 and 2016, their data would also have been wildly out of sync with data reported by neighboring counties:

- a. In 2015, Queens County reported 201 installed wiretaps, with an average of 2.7 extensions per wiretap and an average duration of 100.6 days. In 2016, Queens County reported 79 installed wiretaps, with an average of 2.9 extensions per wiretap and an average total duration of 107.6 days.
- b. In 2015, Bronx County reported 35 installed wiretaps, with an average of 1.3 extensions per wiretap and an average duration of 55.1 days. In 2016, Bronx County reported 13 installed wiretaps, with an average of 1.7 extensions per wiretap and an average duration of 63.6 days.

- c. In 2015, New York County reported 68 installed wiretaps, with an average of 2.3 extensions per wiretap and an average total duration of 95.8 days. In 2016, New York County reported 14 installed wiretaps with an average of 2.7 extensions per wiretap and an average total duration of 91 days.

115. The fact that the Administrative Office Wiretap Reports for Calendar Years 2015 and 2016 reflect that no report was received from KCDA for the two years during which Lenich conducted the illegal wiretap operation is further evidence of the City's policy or custom of deliberate indifference to KCDA wiretap operations.

116. But for a municipal policy or custom of deliberate indifference to the operation of KCDA wiretaps, Defendants Thompson and Gonzalez would not have been permitted to withhold wiretap data from the Administrative Office of U.S. Courts that is required by state and federal law.

117. But for a municipal policy or custom of deliberate indifference to the operation of KCDA wiretaps, it is inconceivable that Lenich could have submitted at least twenty-four forged wiretap orders over the course of eighteen months, authorizing two wiretaps that continued for over well 500 total days, at considerable cost to KCDA, without raising questions about the nature of her "confidential" investigation and the necessity of further surveillance.

118. Despite their actual and/or constructive knowledge that Lenich was conducting unlawful wiretaps for a period of approximately eighteen months, the City and the Supervisory Defendants permitted, tolerated, and were deliberately indifferent to Lenich's conduct, allowing her to intercept and record hundreds, if not thousands, of private oral and electronic communications between Plaintiff and his family members, friends, colleagues and confidential sources.

119. The Supervisory Defendants' deliberate indifference to Lenich's unlawful conduct violated Section 3-1.3 of the National Prosecution Standards, Third Edition, issued by the National District Attorneys Association, which requires prosecutors who become aware that "evidence has been

illegally obtained” to “take affirmative steps to investigate and remediate such problems.” It also violated Section 2.12(f) of the American Bar Association’s Standards on Prosecutorial Investigations, which states that “[t]he prosecutor should stay informed of actions of law enforcement agents and contract personnel throughout the use of non-consensual electronic surveillance and should take appropriate steps to determine whether the required procedures are being followed by those carrying out the surveillance.

Plaintiff’s Substantial Damages

120. Plaintiff has suffered severe emotional distress as a result of the Defendants illegal and tortious conduct. He must live with the knowledge that, for nearly a year and a half, all of his oral and electronic communications were intercepted, recorded, and monitored, including private conversations with his wife and children, his friends, and even confidential sources. His sense of personal security and of trust have been destroyed. Plaintiff can no longer engage in a conversation or exchange text messages or emails without fearing that he is being surveilled. He has even found it difficult to leave the house, due to a paranoia that he is being followed or monitored. He has also been left to wonder to whom his private conversations have been disclosed and lives with the burden of knowing that anyone he speaks to within the NYPD or KCDA may have been informed of details of his private life.

121. The media frenzy caused by the disclosure of the illegal wiretapping scheme, as well as the Individual Defendants’ leaking of illegally obtained information to the press, compounded Plaintiff’s emotional distress and has caused lasting damage to Plaintiff’s relationships, including with his wife and children.

122. Citing sources from within KCDA, including, on information and belief, the Individual Defendants, media reports put Plaintiff, who was married, at the center of a “love triangle” involving both Lenich and Rosenfeld, who is also married. As a result of these leaks, members of the press

harassed Plaintiff and his wife, even staking out their home. Citing sources within the KCDA, including, on information and belief, the Individual Defendants, media reports also incorrectly reported that Plaintiff had threatened Lenich, further damaging his reputation. Even today, an internet search of Plaintiff's name instantly yields extensive negative media coverage as a result of the unlawful conduct of the Defendants.

123. Plaintiff has also suffered consequences at work. Despite being a victim of the illegal wiretapping campaign that was perpetrated on the Supervisory Defendants' watch, they have treated him as a pariah. He was removed from the elite ATF-NYPD Joint Firearms Task Force that he had been selected for and placed on modified duty. Defendant Feldman went so far as to order Plaintiff not to enter the KCDA offices and to remove him from KCDA assignments. As a result, Plaintiff has been deprived of the privileges and opportunities he previously enjoyed, including the use of a take-home car and substantial overtime opportunities.

124. For a year after Lenich's arrest, while Plaintiff was on modified duty, he was deprived of tens of thousands of dollars in overtime pay. These lost past earnings could also impact his pension calculation, thereby having a negative impact on his future earnings in retirement.

125. The reputational harm caused by Defendants' illegal and tortious acts and omissions has also severely limited Plaintiff's prospects for obtaining lucrative employment in the private sector after retirement. Though Plaintiff had long intended to retire and take a high-paying job in the private security industry, he is now virtually unemployable as a result of false and misleading disclosures and negative media coverage resulting from the illegal wiretapping operation.

Plaintiff's Notice of Claim

126. A written notice of claim, sworn by Plaintiff, was served upon Defendants at the Comptroller's Office at 1 Centre Street, New York, New York, on April 30, 2018.

127. Before serving the notice of claim, Plaintiff notified Defendants of his concerns about the illegal wiretapping campaign through the December 21, 2016, letter Plaintiff's counsel sent to the Deputy Chief of Investigation at KCDA, copied to Defendant Schaeffer.

128. Defendants had further notice of Plaintiff's potential claims through the Notice of Claim served by Ms. Rosenfeld on January 27, 2017, within ninety days of the discovery of Lenich's scheme.

129. At least thirty days have elapsed since the service of Plaintiff's Notice of Claim and adjustment or payment of the claim has been neglected or refused.

COUNT ONE

(Electronic Communications Privacy Act, 18 U.S.C. §§ 2510 *et seq.*, 18 U.S.C. §§ 2701, *et seq.*, Against Lenich)

130. Plaintiff repeats and realleges the forgoing paragraphs as if they were fully set forth herein.

131. Lenich intentionally intercepted, used, reviewed, recorded, and disclosed Plaintiff's private electronic and oral communications in a manner that was not authorized by law, in violation of 18 U.S.C. § 2511(1).

132. Lenich also intentionally obtained access to a facility through which Plaintiff's electronic communication service is provided and on which Plaintiff's electronic communications are stored, and thereby obtained Plaintiff's stored electronic communications, in violation of 18 U.S.C. § 2701(a).

133. Lenich acted intentionally in violating Plaintiff's rights under the Wiretap Act and the Stored Communications Act (together, the Electronic Communications Privacy Act or "ECPA").

134. As a direct and proximate result of the violation of Plaintiff's rights under the ECPA, Plaintiff sustained substantial injuries and is entitled to compensatory, statutory, and/or punitive damages as set forth in 18 U.S.C. §§ 2520 and 2707.

COUNT TWO

(Electronic Communications Privacy Act, 18 U.S.C. §§ 2510 *et seq.*, 18 U.S.C. §§ 2701, *et seq.*, Against Thompson, Gonzalez, Schaeffer, Feldman, Donohue, Power, Dowling, Piraino, and Kenavan)

135. Plaintiff repeats and realleges the forgoing paragraphs as if they were fully set forth herein.

136. The Individual Defendants are persons who engaged in the violation of Plaintiff's rights under the ECPA by facilitating the illegal wiretap campaign and/or being deliberately indifferent to it, despite knowing, or having reason to know, that it was unauthorized or illegal.

137. The Supervisory Defendants—Thompson, Gonzalez, Schaeffer, and Feldman—knew or should have known that the wiretaps on Plaintiff's and Stephanie Rosenfeld's cell phones were unauthorized or illegal and yet facilitated them and/or permitted them to continue in violation of the ECPA.

138. Defendant Donohue directly facilitated the violation of Plaintiff's rights under the ECPA by establishing the illegal wiretaps despite knowing, or having reason to know, that they were unauthorized or illegal.

139. The Individual Defendants—Thompson, Gonzalez, Schaeffer, Feldman, Power, Donohue, Dowling, Piraino, and Kenavan—used, reviewed, and/or disclosed Plaintiff's electronic and oral communications, despite knowing that they had been intercepted without Plaintiff's permission and in a manner that was not authorized under law, in violation of the ECPA.

140. The Individual Defendants acted with reckless disregard for Plaintiff's rights under the ECPA.

141. As a direct and proximate result of the violation of Plaintiff's rights under the ECPA, Plaintiff sustained injuries and is entitled to compensatory, statutory, and/or punitive damages as set forth in 18 U.S.C. §§ 2520 and 2707.

COUNT THREE

(Electronic Communications Privacy Act, 18 U.S.C. §§ 2510 *et seq.*, 18 U.S.C. §§ 2701, *et seq.*,
Against the City)

142. Plaintiff repeats and realleges the foregoing paragraphs as if they were fully set forth herein.

143. Lenich intercepted and recorded Plaintiff's oral, wire, and electronic communications while acting in the course of her employment, on City time, and using City equipment, facilities, and funds.

144. The City engaged in the violation of Plaintiff's rights under the ECPA through the actions of its agents and employees, including Lenich and the Individual Defendants, and is responsible for the results of their misconduct under the doctrine of *respondeat superior*.

145. The City is further liable for Lenich's decision to unlawfully intercept Plaintiff's communications through illegal wiretaps because Lenich used her final decision-making authority to carry out the wiretapping campaign. Lenich was a final policymaker with respect to KCDA wiretap campaign generally and with respect to the illegal wiretap campaign specifically. Lenich had final decision-making authority over whether and under what circumstances to conduct a wiretap of Plaintiff's cellular phone and Ms. Rosenfeld's cellular phone, as well as the execution of those wiretaps.

146. The City is further liable for the acts and omissions of Lenich and the Individual Defendants because Lenich's misconduct was directly enabled and facilitated by a municipal policy or custom of deliberate indifference toward the operation of KCDA wiretaps in general and to the illegal wiretap campaign in particular.

147. The City, through KCDA and its agents, including the Individual Defendants, acting under the pretense and color of law, permitted, tolerated, and was deliberately indifferent to the operation of KCDA wiretaps, such that Lenich was able to conduct a months-long "confidential" wiretap campaign without oversight. This longstanding custom or practice allowed wiretaps to proceed

under the authority of a single person, without oversight or periodic checks to verify the validity of the wiretaps, without checking the continued need for the wiretaps after each 30-day period, or confirming continued compliance with wiretap obligations, such as minimization.

148. This deliberate indifference to KCDA wiretap operations generally, and to Lenich's misconduct in particular, constituted a municipal policy, practice, or custom and led to the unlawful interception of Plaintiff's private communications.

149. As a direct and proximate result of the misconduct and abuse of authority described above, Plaintiff sustained injuries and is entitled to statutory damages as set forth in 18 U.S.C. §§ 2520 and 2707.

COUNT FOUR

(42 U.S.C. § 1983/Fourth and Fourteenth Amendments against Lenich)

150. Plaintiff repeats and realleges the foregoing paragraphs as if they were fully set forth herein.

151. By intercepting, searching, reviewing, using, and storing Plaintiff's private communications without cause and without judicial authorization, Lenich deprived Plaintiff of rights, remedies, privileges and immunities guaranteed to every citizen of the United States, secured by 42 U.S.C. § 1983, including, but not limited to, rights guaranteed by the Fourth and Fourteenth Amendments to the United States Constitution to be free from unreasonable searches and seizures.

152. Lenich acted under pretense and color of state law and within the scope of her employment as a KCDA employee. Her actions were taken without authority of law and in abuse of her powers. She acted willfully, knowingly, and with specific intent to deprive Plaintiff of his constitutional rights secured by 42 U.S.C. § 1983 and the Fourth and Fourteenth Amendments to the United States Constitution.

153. As a direct and proximate result of the misconduct and abuse of authority described above, Plaintiff sustained the damages hereinbefore alleged.

COUNT FIVE

(42 U.S.C. § 1983/Fourth and Fourteenth Amendments Against the City)

154. Plaintiff repeats and realleges the foregoing paragraphs as if they were fully set forth herein.

155. Lenich had final decision-making authority over KCDA wiretap operations generally and with respect to the illegal wiretap campaign specifically. Lenich had final decision-making authority over whether and under what circumstances to conduct a wiretap of Plaintiff's cellular phone, as well as the operation of that wiretap.

156. Defendant City is liable for Lenich's decision to unlawfully wiretap Plaintiff's phone because Lenich deliberately chose to conduct an unreasonable search of Plaintiff's phone through the use of an unauthorized wiretap, in violation of his Fourth and Fourteenth Amendment rights, and she had final decision-making authority within the City and the KCDA to carry out her deliberate decision.

157. Defendant City is further liable for the violation of Plaintiff's constitutional rights because the illegal wiretapping campaign was directly enabled and facilitated by a municipal policy or custom of deliberate indifference toward the operation of KCDA wiretaps in general and to the illegal wiretap campaign in particular.

158. The City, through KCDA and its agents, including the Individual Defendants, acting under the pretense and color of law, permitted, tolerated, and was deliberately indifferent to the operation of KCDA wiretaps, such that Lenich was able to conduct a months-long "confidential" wiretap campaign without oversight. This longstanding custom or practice allowed wiretaps to proceed under the authority of a single person, without oversight or periodic checks to verify the validity of the wiretaps, without checking the continued need for the wiretaps after each 30-day period, or confirming continued compliance with wiretap obligations, such as minimization.

159. Defendant City, through the KCDA, acting under the pretense and color of law, permitted, tolerated, and was deliberately indifferent to Lenich's pattern and practice of forging more than a dozen of judicial orders and unlawfully intercepting Plaintiff's electronic communications from at least two cell phones over a eighteen-month period using KCDA equipment, facilities, and funds. This widespread tolerance of Lenich's misconduct constituted a municipal policy, practice, or custom and led to the unlawful search of Plaintiff's private communications.

160. This deliberate indifference to KCDA wiretap operations generally, and to Lenich's misconduct in particular, constituted a municipal policy, practice, or custom and led to the unlawful interception of Plaintiff's private communications.

161. As a direct and proximate result of the City's custom or policy of deliberate indifference, Plaintiff was deprived of his right under the Fourth and Fourteenth Amendments to be free from unreasonable searches and seizures, the damages hereinbefore alleged.

COUNT SIX

(Negligent Retention/Supervision Against the City and Supervisory Defendants)

162. Plaintiff repeats and realleges the foregoing paragraphs as if they were fully set forth herein.

163. At all relevant times, Lenich was employed by Defendant City and supervised by the Supervisory Defendants.

164. The City and the Supervisory Defendants had a duty to protect Plaintiff from having his private communications intercepted, recorded, stored, used, and disclosed by Lenich.

165. The City and the Supervisory Defendants breached that duty by allowing Lenich to intercept, record, store, use, and disclose Plaintiff's private communications.

166. The City and the Supervisory Defendants had reason to know that Lenich posed a threat of abusing her authority over wiretaps because she had a past history of abusing her authority and

harassing co-workers within the KCDA and had demonstrated an interest in ensuring that she could conduct wiretaps more easily without the involvement of the NYPD Tactical Action Response Unit.

167. The City and the Supervisory Defendants knew, or should have known, that Lenich was conducting a months-long illegal wiretapping campaign because Lenich submitted at least twenty-four forged judicial orders, which were reviewed by Defendant Donohue and stored within the KCDA office; she used KCDA equipment, facilities, and funds to conduct her campaign; and she told KCDA employees, including the Supervisory Defendants that she was conducting a confidential law enforcement investigation that they knew, or should have known, did not exist.

168. The Supervisory Defendants were required by state and federal law to keep detailed records on KCDA wiretaps, and yet failed to prevent Lenich from conducting an unauthorized, “confidential” wiretap campaign that lasted several times longer than the average KCDA wiretap and involved at least twenty-four forged judicial orders.

169. As a direct and proximate result of the negligence described above, Plaintiff sustained the damages hereinbefore alleged.

COUNT SEVEN

(Negligence Against the City, Supervisory Defendants, and Donohue)

170. Plaintiff repeats and realleges the foregoing paragraphs as if they were fully set forth herein.

171. The Supervisory Defendants had a duty to ensure that proper protections, policies, and protocols were in place to prevent the unlawful interception of Plaintiff’s private communications by Lenich or any other KCDA employee.

172. The Supervisory Defendants breached that duty by failing to implement and maintain protections, policies, and protocols that would have prevented Lenich from unlawfully wiretapping Plaintiff’s private cell phone, thereby allowing Lenich to intercept, record, store, use, and disclose Plaintiff’s private communications.

173. Donohue had a duty to review the forged judicial orders submitted to him by Lenich to ensure they were not forged.

174. Donohue breached his duty by failing to use reasonable care to notice that the orders Lenich presented to him had forged signatures and lacked the a raised judicial seal, which is standard on valid orders as a means to show their authenticity.

175. The City, as employer of the Supervisory Defendants and Donohue, is responsible for their misconduct under the doctrine of *respondeat superior*.

176. As a direct and proximate result of the misconduct and abuse of authority described above, Plaintiff sustained the damages hereinbefore alleged.

WHEREFORE, Plaintiff requests that the Court grant the following relief jointly and severally against Defendants:

1. Compensatory damages in an amount to be determined at trial for the economic, psychological, and emotional injuries sustained by Plaintiff as a result of the events alleged herein.
2. Punitive damages against the Individual Defendants in an amount to be determined at trial.
3. An order awarding Plaintiff reasonable attorneys' fees, together with the costs of this action.
4. Such other and further relief as the Court may deem appropriate.

Dated: November 26, 2018
New York, New York

WIGGIN AND DANA LLP

/s/ James I. Glasser

James I. Glasser, Esq.
Wiggin and Dana LLP
437 Madison Avenue, 35th Floor
New York, NY 10022
jglasser@wiggin.com
212-490-1700